

Pairwise Relative Primality of Positive Integers

Jerry Hu

A classic result in number theory is that the probability that two positive integers are relatively prime is $6/\pi^2$. More generally the probability that k positive integers chosen arbitrarily and independently are relatively prime is $1/\zeta(k)$, where $\zeta(k)$ is Riemann's zeta function. A short accessible proof of this result was given by J. E. Nymann [3]. In a recent paper L. Tóth [5] solved the problem of finding the probability that k positive integers are pairwise relatively prime by the recursion method, he proved that, for $k \geq 2$, the probability that k positive integers are pairwise relatively prime is

$$A_k = \prod_p \left(1 - \frac{1}{p}\right)^{k-1} \left(1 + \frac{k-1}{p}\right).$$

Given a graph $G = (V, E)$ with $V = \{1, 2, \dots, k\}$, the k positive integers a_1, a_2, \dots, a_k are G -wise relatively prime if $(a_i, a_j) = 1$ for $\{i, j\} \in E$. In this note we consider the problem of finding the probability A_G that k positive integers are G -wise relatively prime.

For a k -tuple positive integers $u = (u_1, u_2, \dots, u_k)$, let $Q_G^{(u)}(n)$ denote the number of k -tuples of positive integers a_1, a_2, \dots, a_k with $1 \leq a_1, a_2, \dots, a_k \leq n$ such that $(a_i, u_i) = 1$ for $i = 1, \dots, k$ and they are G -wise relatively prime.

The next theorem gives an asymptotic formula for $Q_G^{(u)}(n)$ and the exact values of A_G . Before we state the theorem, let us introduce some notations. Given a graph $G = (V, E)$ with $V = \{1, 2, \dots, k\}$, a subset $S \subset V$ is called independent if no two vertices of S are adjacent in G . We denote by $i_m(G)$ the number of independent sets of cardinality m in G , and for a subset $S \subset V$, we denote by $i_{m,S}(G)$ the number of independent sets of cardinality m in G which contains at least one vertex in S . For a k -tuple positive integers $u = (u_1, u_2, \dots, u_k)$, and an integer d , the set of positive integers i with $1 \leq i \leq k$ such that d divides u_i is denoted by $S(u, d)$.

Theorem 1 *For a graph $G = (V, E)$ with $V = \{1, 2, \dots, k\}$, we have uniformly for $n, u_i \geq 1$,*

$$Q_G^{(u)}(n) = A_G f_G(u) n^k + O(\theta(u) n^{k-1} \log^{k-1} n), \quad (1)$$

where

$$A_G = \prod_p \left(\sum_{m=0}^k i_m(G) \left(1 - \frac{1}{p}\right)^{k-m} \frac{1}{p^m} \right),$$

$$f_G(u) = \prod_{p|u_1 u_2 \dots u_k} \left(1 - \frac{\sum_{m=0}^k i_{m,S(u,p)}(G)(p-1)^{k-m}}{\sum_{m=0}^k i_m(G)(p-1)^{k-m}} \right),$$

and if $\theta(u_i)$ denotes the number of square free divisors of u_i , then $\theta(u) = \max\{\theta(u_i), i = 1, 2, \dots, k\}$.

Corollary 2 *The probability that k positive integers a_1, a_2, \dots, a_k are G -wise relatively prime and $(a_i, u_i) = 1$ for $i = 1, \dots, k$ is*

$$\lim_{n \rightarrow \infty} \frac{Q_G^{(u)}(n)}{n^k} = A_G f_G(u).$$

For $u_i = 1$, the probability that k positive integers are G -wise relatively prime is

$$A_G = \prod_p \left(\sum_{m=0}^k i_m(G) \left(1 - \frac{1}{p} \right)^{k-m} \frac{1}{p^m} \right).$$

In [2], P. Moree proposed the problems of finding probabilities that k positive integers have exact (or at least) r relatively prime pairs. Using Theorem 1 and an Inclusion-Exclusion formula in combinatorics (see exercise 1 of chapter 2 in [4]), we can give a solution to his problems.

Corollary 3 *The probability that k positive integers have exactly r relatively prime pairs is*

$$A_{k,=r} = \sum_{i=r}^{k(k-1)/2} (-1)^{i-r} \binom{i}{r} B_{k,i},$$

and the probability that k positive integers have at least r relatively prime pairs is

$$A_{k,\geq r} = \sum_{i=r}^{k(k-1)/2} (-1)^{i-r} \binom{i-1}{r-1} B_{k,i},$$

where

$$B_{k,i} = \sum_{|E|=i} A_G.$$

In particular, the probability that k positive integers are pairwise not relatively prime is

$$A_{k,=0} = \sum_{i=0}^{k(k-1)/2} (-1)^i B_{k,i}.$$

In [1], J. L. Fernández and P. Fernández proved that the number of relatively prime pairs is asymptotically normal as k tends to ∞ .

To prove Theorem 1 we need the following lemmas.

Lemma 4 For $k, n \geq 1$, a graph $G = (V, E)$ with $V = \{1, 2, \dots, k+1\}$, and $u = (u_1, u_2, \dots, u_{k+1})$ with $u_i \geq 1$,

$$Q_G^{(u)}(n) = \sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n Q_{G-v}^{(j*u)}(n),$$

where $G-v$ is the graph obtained from G by deleting the vertex $v=k+1$ together with all the edges incident to v , and if $(j*u)_i$ denotes the i th component of $j*u$, then

$$(j*u)_i = \begin{cases} ju_i & \text{if } i \text{ is adjacent to } v \text{ in } G, \\ u_i & \text{otherwise,} \end{cases}$$

for $i = 1, 2, \dots, k$.

Proof. The $k+1$ positive integers a_1, a_2, \dots, a_{k+1} are G -wise relatively prime and $(a_i, u_i) = 1$ for $i = 1, 2, \dots, k+1$ if and only if the first k positive integers a_1, a_2, \dots, a_k are $(G-v)$ -wise relatively prime and $(a_i, u_i) = 1$ for $i = 1, 2, \dots, k$, and $(a_i, a_{k+1}) = 1$ when the vertex i is adjacent to the vertex $v = k+1$, and $(a_{k+1}, u_{k+1}) = 1$. We have

$$Q_G^{(u)}(n) = \sum_{\substack{a_{k+1}=1 \\ (a_{k+1}, u_{k+1})=1}}^n Q_{G-v}^{(a_{k+1}*u)}(n) = \sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n Q_{G-v}^{(j*u)}(n).$$

Lemma 5 For $k, u_i \geq 1$, a graph $G = (V, E)$ with $V = \{1, 2, \dots, k\}$, and S a subset of vertices in V ,

$$\frac{f_G(j*u)}{f_G(u)} = \sum_{d|j} \frac{\mu(d)\alpha_{G,S}(u, d)}{\alpha_G(u, d)},$$

if d is square free, then

$$\frac{\alpha_{G,S}(u, d)}{\alpha_G(u, d)} \leq \frac{k^{\omega(d)}}{d},$$

where

$$\alpha_G(u, d) = \prod_{p|d} \left(\sum_{m=0}^k i_m(G - S(u, p))(p-1)^{k-m} \right),$$

$$\alpha_{G,S}(u, d) = \prod_{p|d} \left(\sum_{m=0}^k i_{m,S}(G - S(u, p))(p-1)^{k-m} \right),$$

and if $(j*u)_i$ denotes the i th component of $j*u$, then

$$(j*u)_i = \begin{cases} ju_i & \text{if } i \text{ is in } S, \\ u_i & \text{otherwise,} \end{cases}$$

for $i = 1, 2, \dots, k$, and $\omega(d)$ denote the number of distinct prime factors of d .

Proof. It suffices to verify the equality for $j = p^a$ a prime power:

$$\begin{aligned}
& \sum_{d|p^a} \frac{\mu(d)\alpha_{G,S}(u, d)}{\alpha_G(u, d)} \\
&= 1 - \frac{\sum_{m=0}^k i_{m,S}(G-S(u, p))(p-1)^{k-m}}{\sum_{m=0}^k i_m(G-S(u, p))(p-1)^{k-m}} \\
&= \frac{\sum_{m=0}^k i_m(G-S(u, p))(p-1)^{k-m} - \sum_{m=0}^k i_{m,S}(G-S(u, p))(p-1)^{k-m}}{\sum_{m=0}^k i_m(G-S(u, p))(p-1)^{k-m}} \\
&= \frac{\sum_{m=0}^k i_m(G)(p-1)^{k-m} - \sum_{m=0}^k i_{m,S \cup S(u, p)}(G)(p-1)^{k-m}}{\sum_{m=0}^k i_m(G)(p-1)^{k-m} - \sum_{m=0}^k i_{m,S(u, p)}(G)(p-1)^{k-m}} \\
&= \frac{f_G(p^a * u)}{f_G(u)}.
\end{aligned}$$

Now we prove the inequality. Notice that

$$i_0(G-S(u, p)) = 1, \quad i_{0,S}(G-S(u, p)) = 0, \quad i_{m,S}(G-S(u, p)) \leq i_m(G-S(u, p)).$$

Then when d is square free,

$$\begin{aligned}
\frac{\alpha_{G,S}(u, d)}{\alpha_G(u, d)} &= \prod_{p|d} \frac{\sum_{m=0}^k i_{m,S}(G-S(u, p))(p-1)^{k-m}}{\sum_{m=0}^k i_m(G-S(u, p))(p-1)^{k-m}} \\
&\leq \prod_{p|d} \frac{\sum_{m=1}^k i_m(G-S(u, p))(p-1)^{k-m}}{(p-1)^k + \sum_{m=1}^k i_m(G-S(u, p))(p-1)^{k-m}} \\
&\leq \prod_{p|d} \frac{\sum_{m=1}^k \binom{k}{m} (p-1)^{k-m}}{(p-1)^k + \sum_{m=1}^k \binom{k}{m} (p-1)^{k-m}} \\
&= \prod_{p|d} \frac{(p^k - (p-1)^k)}{p^k} \\
&\leq \prod_{p|d} \frac{kp^{k-1}}{p^k} \\
&= \prod_{p|d} \frac{k}{p} = \frac{k^{\omega(d)}}{d}
\end{aligned}$$

For the proof of the theorem, we proceed by induction on k . For $k = 1$, we have by the Inclusion-Exclusion Principle

$$Q_{\{1\}}^{(u_1)}(n) = \sum_{\substack{j=1 \\ (j, u_1) = 1}}^n 1 = \sum_{d|u_1} \mu(d) \lfloor \frac{n}{d} \rfloor = \sum_{d|u_1} \mu(d) \left(\frac{n}{d} + O(1) \right)$$

$$= n \sum_{d|u_1} \frac{\mu(d)}{d} + O\left(\sum_{d|v} \mu^2(d)\right).$$

Hence,

$$Q_{\{1\}}^{(u_1)}(n) = \sum_{\substack{j=1 \\ (j, u_1)=1}}^n 1 = n \frac{\phi(u_1)}{u_1} + O(\theta(u_1)) \quad (2)$$

and (1) is true for $k = 1$ with $A_{\{1\}} = 1$, $f_{\{1\}}(u_1) = \frac{\phi(u_1)}{u_1}$, ϕ denoting the Euler function.

Suppose that (1) is valid for k , we prove it for $k+1$. Let $u = (u_1, u_2, \dots, u_{k+1})$ and $u' = (u_1, u_2, \dots, u_k)$, from Lemma 4 we have

$$\begin{aligned} Q_G^{(u)}(n) &= \sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n Q_{G-v}^{(j*u)}(n) \\ &= \sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n A_{G-v} f_{G-v}(j*u) n^k + O(\theta(j*u) n^{k-1} \log^{k-1} n) \\ &= A_{G-v} f_{G-v}(u') n^k \sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n \frac{f_{G-v}(j*u')}{f_{G-v}(u')} \\ &\quad + O(\theta(u') n^{k-1} \log^{k-1} n \sum_{j=1}^n \theta(j)). \end{aligned} \quad (3)$$

Here $\sum_{j=1}^n \theta(j) \leq \sum_{j=1}^n \tau_2(j) = O(n \log n)$, where $\tau_2 = \tau$ is the divisor function.

Furthermore, in Lemma 5 choosing the subset S to be the open neighbourhood $N(v)$ of v , which is the set of vertices adjacent to v , we have

$$\begin{aligned} &\sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n \frac{f_{G-v}(j*u')}{f_{G-v}(u')} \\ &= \sum_{\substack{de=j \leq n \\ (j, u_{k+1})=1}} \frac{\mu(d) \alpha_{G-v, N(v)}(u', d)}{\alpha_{G-v}(u', d)} \\ &= \sum_{\substack{d \leq n \\ (d, u_{k+1})=1}} \frac{\mu(d) \alpha_{G-v, N(v)}(u', d)}{\alpha_{G-v}(u', d)} \sum_{\substack{e \leq \frac{n}{d} \\ (e, u_{k+1})=1}} 1 \end{aligned}$$

Using (2), we have

$$\sum_{\substack{j=1 \\ (j, u_{k+1})=1}}^n \frac{f_{G-v}(j*u')}{f_{G-v}(u')}$$

$$\begin{aligned}
&= \sum_{\substack{d \leq n \\ (d, u_{k+1}) = 1}} \frac{\mu(d) \alpha_{G-v, N(v)}(u, d)}{\alpha_{G-v}(u', d)} \left(\frac{\phi(u_{k+1})}{u_{k+1}} \frac{n}{d} + O(\theta(u_{k+1})) \right) \\
&= \frac{\phi(u_{k+1})}{u_{k+1}} n \sum_{\substack{d \leq n \\ (d, u_{k+1}) = 1}} \frac{\mu(d) \alpha_{G-v, N(v)}(u', d)}{d \alpha_{G-v}(u', d)} + O \left(\theta(u_{k+1}) \sum_{d \leq n} \frac{k^{\omega(d)}}{d} \right), \quad (4)
\end{aligned}$$

by Lemma 5.

Hence, the main term of (4) is

$$\begin{aligned}
&\frac{\phi(u_{k+1})}{u_{k+1}} n \sum_{\substack{d=1 \\ (d, u_{k+1})=1}}^{\infty} \frac{\mu(d) \alpha_{G-v, N(v)}(u', d)}{d \alpha_{G-v}(u', d)} \\
&= \frac{\phi(u_{k+1})}{u_{k+1}} n \prod_{p \nmid u_1 u_2 \cdots u_k u_{k+1}} \left(1 - \frac{\sum_{m=0}^k i_{m, N(v)}(G-v)(p-1)^{k-m}}{p \left(\sum_{m=0}^k i_m(G-v)(p-1)^{k-m} \right)} \right) \\
&\quad \prod_{\substack{p \mid u_1 u_2 \cdots u_k \\ p \nmid u_{k+1}}} \left(1 - \frac{\sum_{m=0}^k i_{m, N(v)}(G-v-S(u, p))(p-1)^{k-m}}{p \left(\sum_{m=0}^k i_m(G-v-S(u, p))(p-1)^{k-m} \right)} \right) \\
&= n \prod_p \left(1 - \frac{\sum_{m=0}^k i_{m, N(v)}(G-v)(p-1)^{k-m}}{p \left(\sum_{m=0}^k i_m(G-v)(p-1)^{k-m} \right)} \right) \\
&\quad \prod_{p \mid u_{k+1}} \left(1 - \frac{1}{p} \right) \prod_{p \mid u_1 u_2 \cdots u_{k+1}} \left(1 - \frac{\sum_{m=0}^k i_{m, N(v)}(G-v)(p-1)^{k-m}}{p \left(\sum_{m=0}^k i_m(G-v)(p-1)^{k-m} \right)} \right)^{-1} \\
&\quad \prod_{\substack{p \mid u_1 u_2 \cdots u_k \\ p \nmid u_{k+1}}} \left(1 - \frac{\sum_{m=0}^k i_{m, N(v)}(G-v-S(u, p))(p-1)^{k-m}}{p \left(\sum_{m=0}^k i_m(G-v-S(u, p))(p-1)^{k-m} \right)} \right),
\end{aligned}$$

and its O-terms are

$$\begin{aligned}
O\left(n \sum_{d > n} \frac{k^{\omega(d)}}{d^2}\right) &= O\left(n \sum_{d > n} \frac{\tau_k(d)}{d^2}\right) \\
&= O(\log^{k-1} n)
\end{aligned}$$

by Lemma 3(b) in [5], which gives an asymptotic estimate of the sum

$$\sum_{n > x} \frac{\tau_k(n)}{n^2} = O\left(\frac{\log^{k-1} x}{x}\right)$$

and

$$\begin{aligned}
O(\theta(u_{k+1}) \sum_{d \leq n} \frac{k^{\omega(d)}}{d}) &= O(\theta(u_{k+1}) \sum_{d \leq n} \frac{\tau_k(d)}{d}) \\
&= O(\theta(u_{k+1}) \log^k n)
\end{aligned}$$

from Lemma 3(a) in [5], which gives an asymptotic estimate of the sum

$$\sum_{n \leq x} \frac{\tau_k(n)}{n} = O(\log^k x).$$

Substituting into (3), we get

$$\begin{aligned}
Q_G^{(u)}(n) &= A_{G-v} \prod_p \left(1 - \frac{\sum_{m=0}^k i_{m,N(v)}(G-v)(p-1)^{k-m}}{p(\sum_{m=0}^k i_m(G-v)(p-1)^{k-m})} \right) \\
&\quad f_{G-v}(u) \prod_{p|u_{k+1}} \left(1 - \frac{1}{p} \right) \prod_{p|u_1 u_2 \dots u_{k+1}} \left(1 - \frac{\sum_{m=0}^k i_{m,N(v)}(G-v)(p-1)^{k-m}}{p(\sum_{m=0}^k i_m(G-v)(p-1)^{k-m})} \right)^{-1} \\
&\quad \prod_{\substack{p|u_1 u_2 \dots u_k \\ p \nmid u_{k+1}}} \left(1 - \frac{\sum_{m=0}^k i_{m,N(v)}(G-v-S(u,p))(p-1)^{k-m}}{p(\sum_{m=0}^k i_m(G-v-S(u,p))(p-1)^{k-m})} \right) n^{k+1}, \\
&\quad + O(n^k \log^{k-1} n) + O(\theta(u_{k+1}) n^k \log^k n) + O(\theta(u') n^k \log^k n) \\
&= A_G f_G(u) n^{k+1} + O(\theta(u) n^k \log^k n)
\end{aligned}$$

by a simple computation, which shows that the formula is true for $k+1$ and we complete the proof.

T. Freiberg computed the probability that three positive integers are pairwise not relatively prime, see [2]. As an application of our method, we compute the probability that four positive integers are pairwise not relatively prime.

Let $A_{3,i}$ denote the probability that three positive integers have i relatively prime pairs, for $i = 1, 2, 3$. By Theorem 1 and Corollary 3, we have

$$\begin{aligned}
A_{3,0} &= 1, \quad A_{3,1} = \prod_p \left(1 - \frac{1}{p^2} \right), \quad A_{3,2} = \prod_p \left(1 - \frac{1}{p} \right) \left(1 + \left(1 - \frac{1}{p} \right) \frac{1}{p} \right), \\
A_{3,3} &= \prod_p \left(1 - \frac{1}{p} \right)^2 \left(1 - \frac{2}{p} \right),
\end{aligned}$$

and

$$A_{3,0} = 1 - 3A_{3,1} + 3A_{3,2} - A_{3,3}.$$

This recovers T. Freiberg's result.

When $k = 4$, the number of graphs with given number of edges and the number of independent sets are summarized in the following table.

number of edges	number of graphs	number of independent sets
0	1	$i_2(G) = 6, i_3(G) = 4, i_4(G) = 1$
1	6	$i_2(G) = 6, i_3(G) = 4, i_4(G) = 1$
2	type I: 12	type I: $i_2(G) = 4, i_3(G) = 2, i_4(G) = 0$
	type II: 3	type II: $i_2(G) = 4, i_3(G) = 0, i_4(G) = 0$
3	type I: 4	type I: $i_2(G) = 3, i_3(G) = 1, i_4(G) = 0$
	type II: 16	type II: $i_2(G) = 3, i_3(G) = 0, i_4(G) = 0$
4	15	$i_2(G) = 2, i_3(G) = 0, i_4(G) = 0$
5	6	$i_2(G) = 1, i_3(G) = 0, i_4(G) = 0$
6	1	$i_2(G) = 0, i_3(G) = 0, i_4(G) = 0$

Given graph G with four vertices and i edges, let $A_{4,i}$ denote the probability that integers are G -wise relatively prime for $i = 1, 2, \dots, 6$, if there are more than one type of graphs with fixed number of edges i , for the graphs of type j , the probability is denoted by $A_{4,i,j}$. Again by Theorem 1 and Corollary 3, we have

$$A_{4,0} = 1, A_{4,1} = \prod_p \left(1 - \frac{1}{p^2}\right), \quad A_{4,2,1} = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \left(1 - \frac{1}{p}\right) \frac{1}{p}\right),$$

$$A_{4,2,2} = \prod_p \left(1 - \frac{1}{p^2}\right)^2, \quad A_{4,3,1} = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \left(1 - \frac{1}{p}\right)^2 \frac{1}{p}\right),$$

$$A_{4,3,2} = \prod_p \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{2}{p}\right), \quad A_{4,4} = \prod_p \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p} - \frac{1}{p^2}\right),$$

$$A_{4,5} = \prod_p \left(1 - \frac{1}{p}\right)^2 \left(1 + 2 \left(1 - \frac{1}{p}\right) \frac{1}{p}\right), \quad A_{4,6} = \prod_p \left(1 - \frac{1}{p}\right)^3 \left(1 + \frac{3}{p}\right),$$

and

$$A_{4,=0} = 1 - 6A_{4,1} + 12A_{4,2,1} + 3A_{4,2,2} - 4A_{4,3,1} - 16A_{4,3,2} + 15A_{4,4} - 6A_{4,5} + A_{4,6}.$$

References

- [1] J. L. Fernández, P. Fernández, *Asymptotic normality and greatest common divisor*, arXiv:1302.2357 [mathPR], Feb. 2013.
- [2] P. Moree, *Counting carefree couples*, arXiv:math/0510003 [math.NT], Sep. 2005.
- [3] J. E. Nymann, *On the probability that k positive integers are relatively prime*, J. Number Theory 4 (1972), 469-473.
- [4] R. Stanley, *Enumerative Combinatorics*, Volume 1, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1997.

- [5] L. Tóth, *The probability that k positive integers are pairwise relatively prime*, Fibonacci Quart. 40 (2002), 13-18.

Department of Mathematics and Computer Science, School of Arts & Sciences, University of Houston-Victoria, 14000 University Blvd, Sugar Land, TX 77479, USA